Journal of Engineering and Applied Sciences 13 (18): 7708-7715, 2018
ISSN: 1816-949X

Performance Enhancement of Image Encryption By Using BK-Cube Network Design

[1]Ashwaq T. Hashim and [2]Yossra H. Ali
[1]Department of Control and Systems Engineering,
[2]Department of Computer Sciences, University of technology, Baghdad, Iraq

Abstract: This study introduces some new criteria that can be used for enhancing the design of some known standard block ciphers for image encryption. It designed to meet the requirements of increased security and better performance. One new feature of proposed BK-Cube network algorithm is used a cube network design where the cube looking composition of F-functions is used instead of rounds. The BK-Cube design is a Type-3 Feistel network that takes three inputs and produces three outputs with some additional integer parameters which is represented the used sub-keys. A round of some existing block cipher has been used as a function on the new BK-Cube design of proposed system. The block size of the proposed system is 875 bits if 128 bits encryption algorithm is used while 448 bits when used 64 bits encryption algorithm. The key size of proposed system is 128 bits. E8-chained encryption utilized for subkeys generation. Then a recursion has been used to generate required subkeys. Results are analyzed to confirm that the new design has been enhanced the performance of the some existing block ciphers for image encryption with respect to information system security.

Key words: Cryptography, block cipher, Type-3 Feistel network, Cube network, image encryption, proposed system

INTRODUCTION

Rabid growth has enabled computer networks transfer large files such as digital photos, easy over the internet (Singh *et al*., 2013). Security for text data is commonly achieved through the use of data encryption. Because of the huge data and real time limitations, algorithms that are good for text data may not be appropriate for multimedia data. In most natural images, the values of the neighboring pixels are strongly correlated (i.e., reasonably prediction for a value of any given pixel from the values of its neighbors) (Gonzales and Woods, 2002).

For decorrelating the high correlation among pixels and increase the entropy value, the proposed algorithm splits the image into blocks and then shuffles their positions before it passes them to the proposed Bk-Cube network design. The correlation and entropy security measurements have been used and the results showed that the proposed system decreased correlation and increased entropy value when compared to using existing of block ciphers which are tested and thus, the level of security is strengthen for these images.

At present, two major keys exits to increase decorrelate image pixels and increase security the first one by increasing the input block size and scrambling the image pixels randomly.

Literature review: By Helal and Hashim (2010) analyzed RC6 with two modified version 512 and 640 bits RC6-Cascade encryption algorithms to investigate the encryption efficiency for them to digital images and providing a new mathematical measure for encryption efficiency. With most of the measuring factors, RC6-Cascade achieved the best result on images of binary data. By Sudha and Divya (2015) executed an image securely with a Blowfish algorithm from the perspective of cryptology. Blowfish is used for the applications where the key doesn't change often and has a larger space to store the data. By Padate and Patel (2015) described a design of effective security for communication by AES algorithm to encrypt and decrypt. It is based on key expansion of the AES in which a bit wise exclusive or operation of a set of pixels of image are used in the encryption process along with the a 128 bits key that changes per set of pixels. The results showed that, the time required for encryption by AES algorithm is less than

Corresponding Author: Ashwaq T. Hashim, Department of Control and Systems Engineering, University of Technology, Baghdad, Iraq

the time required by DES algorithm and due to these features the algorithm is appropriate for image encryption in applications of real time. By Alshahrani and Walker (2015) illustrated a symmetric block cipher cryptography algorithm. The system utilized an 8×8×8 cube and each cell contents a pair of binary inputs. The cube can provide a large number of combinations that can produce a very powerful algorithm and a long key size. Because of the fast technique and lightweight used in this idea, it is expected to be extremely fast compared to the majority of current algorithms such as DES and AES. By Ali and Ressan (2016) proposed algorithm for images protection depended on serpent block. In modified serpent, a type three feistel network has been used and the block size is increased to 512 bits. The correlation coefficient decreases to below the traditional serpent algorithm. By Shrivastava and Singh (2016) introduced an image cryptography system based on RC6. The key size and variable numbers of rounds made RC6 more secure. The size of key is variable and up to 2040 bits. The results are investigated depends on the entropy and correlation coefficients.

MATERIALS AND METHODS

Block ciphers: Encryption based symmetric key, commonly named secret or traditional encryption, points to the kinds of encryption where encryption and decryption were used similar key values. Further, encryption based symmetric key consist of a stream and block ciphers; The block cipher is used in this research. The idea of a block cipher is to split the text into fairly bulky blocks, for example, 128 bits and then encodes every block individually (Helal and Hashim, 2010). Some of existing block ciphers are described in next sections.

RC6: One of the finalists in the Advanced Encryption Standard (AES) competition is a block cipher algorithm RC6. It is an extension to its predecessor RC5. Differences will be noted consequently as result of development RC6 from RC5. The RC6 has a 128-bits block size and supports key sizes of 128, 192 and 256 bits up to 2040 bits.

Three components such as the key expansion algorithm, the encryption algorithm and the decryption algorithm comprise RC6. The parameter is viewed in the following specification: RC6-w/r/b where w is the size of word, r is the non-negative number of rounds and b is the length in byte of the encryption key. A data-dependent rotations is used in the RC6 and it is on basis on seven primitive operations which are shown in Table 1. Normally, there are only six primitive operations; However, the parallel assignment is primitive and a basic

Table 1: RC6 operations

Operation	Description
a+b	Addition of integer mod 2^w
a–b	Subtraction of mod 2^w
a⊕b	Bitwise XOR of w-bit words
a×b	Multiplication of integer mod 2^w
a<<<b	The w-bit word a is rotated to the left by the amount given by the least significant ($\log_2$ w) bits of b
a>>>b	The w-bit word a is rotated to the right by the amount given by the least significant ($\log_2$ w) bits of b
Enc: (A, B, C, D) = (B, C, D, A)	Values on the right to registers on the
Dec: (A, B, C, D) = (D, A, B, C)	left parallel assignment

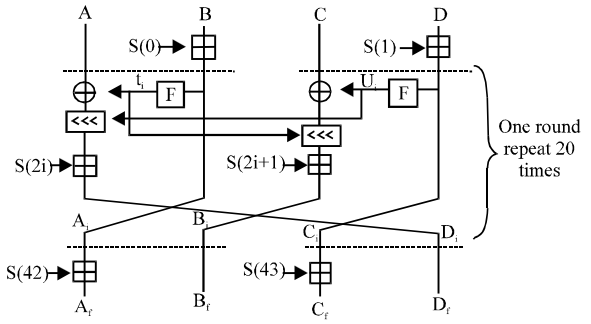

Fig. 1: Overall structure of the RC6 algorithm

operation to RC6. The subtraction, addition and multiplication operations use two's complement representations. Integer multiplication is utilized to increase diffusion per round and increase the speed of the cipher. Figure 1 is the overall structure of the RC6 encryption process.

Advanced Encryption Standard (AES): A symmetric block cipher AES utilized the same key for both encryption and decryption. The algorithm Rijndael is a variable block and key sizes. The block and key can be any length from 128, 160, 192, 224, 256 bits and may not be the same. However, the block size of the standard AES algorithm can only of 128 bits and the keys-128, 192, 256 bits can be chosen. The name of AES algorithm is modified to AES-128, AES-192 or AES-256, respectively depending on which version is used.

The number of rounds of AES depends on length key. For example, if 128 bit key length is used then the number of rounds is 10 while the rounds are 12 and 14 for 192 and 256 bits, respectively. The 128 bit key size is the most common key length likely to be utilized. The overall structure of AES can be seen in Fig. 2 (Hernandez *et al*., 2001).

Blowfish: By Schneier (1996) introduced a fast eencryption algorithm called Blowfish which is freely avalible replacemnt. This method is widely studies, since,

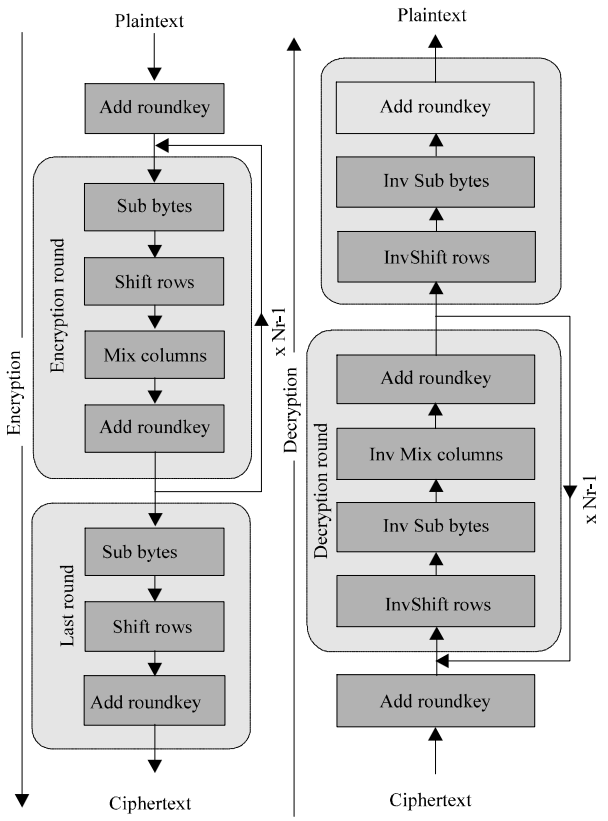

Fig. 2: Overall structure of the AES algorithm

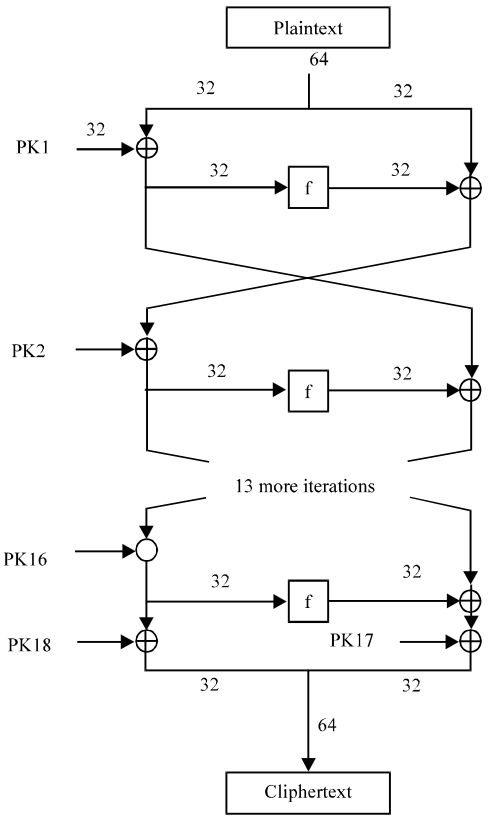

Fig. 3: Overall structure of the Blowfish algorithm

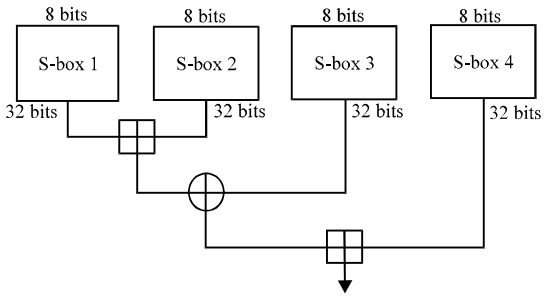

Fig. 4: F function of the Blowfish algorithm

then slowly increasing in popularity. The Blowfish algorithm has many advantages. It is efficient and sutiable implemented by hardware design and no license is needed. The basic operators of Blowfish algorithm involve addition, XOR and lookup tables. These tables are four S-boxes and P-array. Blowfish is Feistel network and the design of the function used is equal to simplifying the fundementals required in the DES to ensure equivalent security to maintain high speed and efficiency in software.

Blowfish is a 64 bits block cipher and takes a variable-length key, from 32-448 bits,. Blowfish is a fast algorithm and can encrypt data on 32 bits microprocessors. Figure 3 and 4 show the the structure of blowfish algorithm and F-function design, respecively (Rivest *et al*., 1998).

The Tiny Encryption Algorithm (TEA): The Tiny Encryption Algorithm (TEA) is a block cipher known as a simple of description and easy to implement. This cipher was firstly introduced by Wheeler and Needham. TEA researches on 64 bits plaintext at a time and using 128 bits key. It is a Feistel network of 64 rounds, typically applied on pairs termed rounds.The key schedule was very simple. It exactly mixed all of the main material for each round in the same way. Various multiples of a magic constant is utilized to deny simple attacks based on the symmetry of the rounds. The magic constant, 2654435769 or 9E3779B916 has been chosen to be 232φ where φ was the golden ratio.

TEA is a Feistel cipher which utilizes various (orthogonal) algebraic groups XOR, ADD and SHIFT in this instance. This is a truly ingenious way of saving Shannon's twin characteristic of confusion and diffusion which are required to a secure block cipher without needing the explicitly of P-boxes and S-boxes, respectively. Figure 5 shows the structure of TEA algorithm.

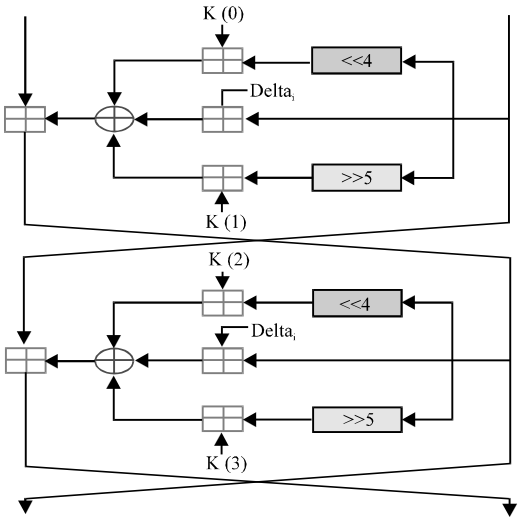

Fig. 5: Overall structure of the TEA algorithm

RESULTS AND DISCUSSION

Proposed system: The input image to the proposed system has been scrambled into 7 subblocks randomly (i.e., depending on the number of inputs to the proposed system). The purpose of this step is to decorrelate adjacent pixels of input images. Figure 6 shows the block diagram of scrambled image. After that the resulted blocks are passed to BK-Cube network algorithm where cube looking composition of F-functions is used instead of rounds as shown in Fig. 7. The BK-Cube design ofproposed algorithm is a Type-3 Feistel network that takes three inputs and produces three outputs with some additional integer parameters which is represented the used subkeys. Figure 8 shows the block diagram of proposed BK design.

The block size of the proposed system is variable depending on the function that has been used in the Bk-Cube network algorithm. If the function is a round of the AES or RC6 encryption algorithm have been used the input are 875 bits plaintext (i.e., X_1, ..., X_7 of 128 bits blocks each one from scrambled subblocks). On the other hand the input block size is 448 when blowfish or TEA encryption algorithm have been used (i.e., X_1, ..., X_7 of 64 bits blocks each one from scrambled subblocks).

Algorithm 1: Image encryption

Input: Plain color image//RGB Bitmap Image
Output: Encrypted image
Step 1: Load image I
Step 2: Scrambled image *I* using Algorithm 2
Step 3: Pass scramble subblocks to the Algorithm 3
Step 4: output Encrypted image

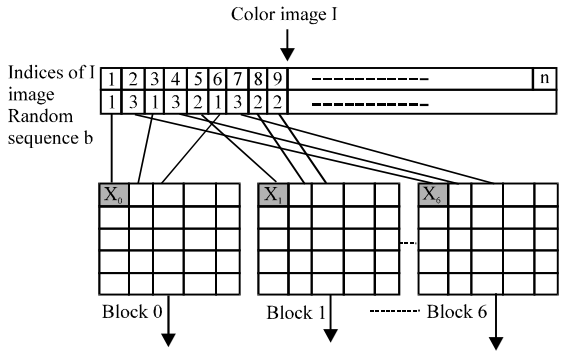

Fig. 6: Scramble image into 7 subblocks

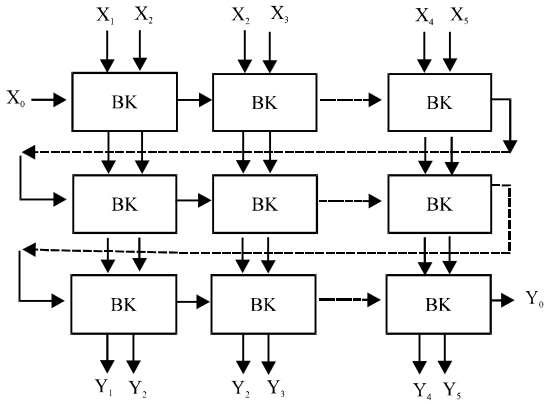

Fig. 7: The block diagram of the proposed BK-Cube network design

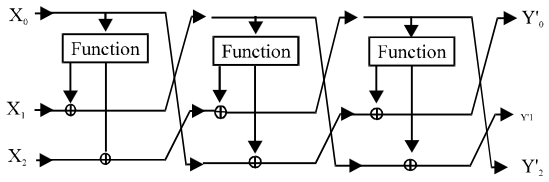

Fig. 8: The proposed BK design

Algorithm 2: Scrambling Color Image

Input: Plain color image
Output: Scrambled seven blocks Y_i i = 0, ..., 6
Step 1: Initialize b as a sequence of length n:
Step 1.1: For I = 1→n//where n is the length of image
b (I) = I mod k//k is the number of blocks
end loop I
Step 1.2 : Let J = R_1
Step 1.3: for I = n-1→1
J = (R_2 × j + R_3) mod I
//R_1, R_2 and R_3 are three large prime numbers
Swap b (I), b (J)
End loop I
Step 2: Divide I color image into k blocks
For j =1→n
z = b (j)
If (z<>0)
z = z×n / k
no = count (z)+1
x = z+no
blocks (x) = I (j)
End loop I
Step 3: output scrambled seven Subblocks Y_i , i = 0, ..., 6

Table 2: The algorithms factors

Algorithms	Block size (bits)	Key length (bits)
Blowfish	64	128
TEA	64	128
RC6	128	128
AES	128	128

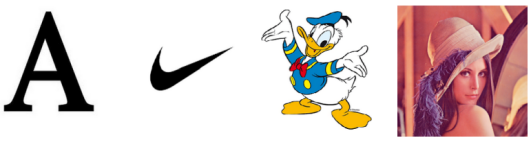

Fig. 9: Test images

Algorithm 3: BK-Cube network
Input: Scrambled Subblocks
Output: Encrypted image
Step 1: Take seven 128-bit block X_i from subblock where i = 0..,6
Step 2: Pass the first three 128 bits blocks to the BK
Step 3: The three outputs from *Bk* passed to next of the Bk_s
Step 4: Repeat step 2, 3 for three times
Step 5: Repeat step 1-4 for all image blocks

Subkeys generations: The input key size of proposed system is 128 bits. Three rounds have been required in each proposed Bk-Cube network design. Each round required 128 bits in RC6 and AES encryption algorithms while 128 bits key have been required in two rounds of TEA algorithm. In other hand the Blowfish algorithm has used 128 bits key in four rounds. E8-chained encryption utilized for subkeys generation. Let key be an inserted key. Then a recursion has been used to generate required subkeys such as following:

$$K_0 = K, K_1 = E_8(K_0), \ldots, K_i = E_8(K_{i-1}), \ldots, K_8 = E_8(K_9)$$

Statistical analysis: Statistical analyses are applied to investigate the characteristics of the confusion and diffusion of the proposed system. The experimental results illustrate that the system immunize against the statistical attacks. This is done by testing the statistical distribution of the pixel values of the encrypted images, the degree of correlation between the plain and cipher images and the information entropy. Table 2 lists the algorithm factors of using algorithms in experimental tests.

Statistical security analysis: This study presents the tests are conducted to assess the efficiency and security of the proposed system. These tests include visual tests. For visual testing four color images of 256×256 pixels are used. Figure 9 show the test images which are A, Nike, Duck and Lena images.

The images encrypted of the test images using the Blowfish, Tea, RC6 and AES encryption algorithms are showed in the Fig. 10-13, respectively. While

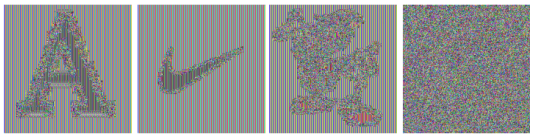

Fig. 10: Encrypted images using Blowfish algorithm

Fig. 11: Encrypted images using TEA algorithm

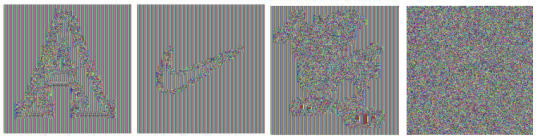

Fig. 12: Encrypted images using RC6 algorithm

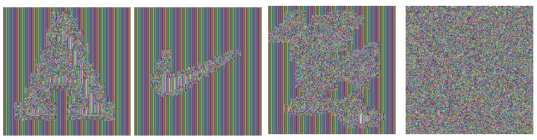

Fig. 13. Encrypted images using AES algorithm

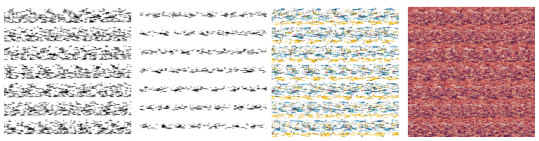

Fig. 14: Scrambled images after performed proposed random algorithm

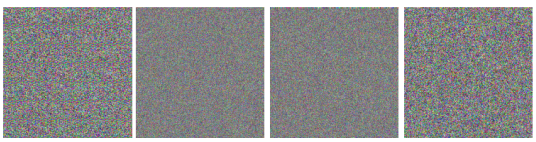

Fig. 15: Encrypted images after performed proposed system with Blowfish as function

Fig. 14 depicts the scrambled images after applying proposed random function and Fig. 15-18 depict images when applying proposed BK-network design system with Blowfish, TEA, RC6 and AES as function of the system.

From these figures, one can notice that there is no resembling of sensory perception between original images

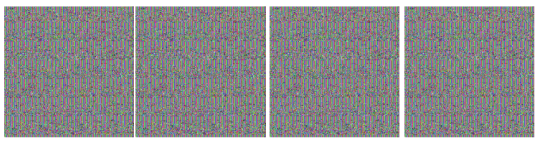

Fig. 16: Encrypted images after performed proposed system with TEA as function

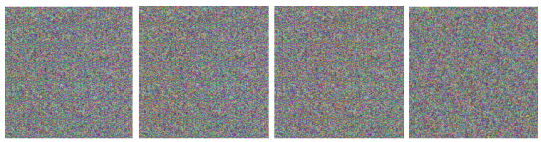

Fig. 17: Encrypted images after performed proposed system with RC6 as function

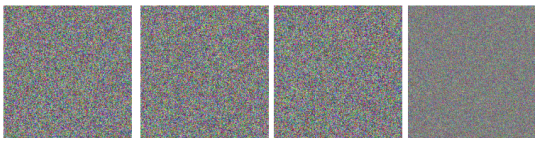

Fig. 18: Encrypted images after performed proposed system with AES as function

and their ciphered counterparts with proposed algorithm while with Blowfish, TEA, RC6 and AES encryption algorithms still some information can be inferred from the encrypted images, so that, the conclusion is drawn on about the appearance of the image. The encrypted image must differ significantly from its original form.

Correlation: A relationship between two sets of variables is measured by correlation. The cross correlation coefficient utilized in this research has following Eq. 1 (Rivest *et al*., 1998):

$$C = \frac{n\sum_i x_i y_i - \sum_i x_i \sum_i y_i}{\sqrt{\left(\sum_i x_i^2\right) - \left(\sum_i y_i^2\right)}} \quad (1)$$

Where:

C = The cross correlation coefficient
n = The number of pixels of image
$\{x_i\}$ = Pixels values of the original image
$\{y_i\}$ = Pixels values of the cipher image (Rivest *et al*., 1998)

Tables 3-6 show the correlation between original images and ciphered images using Blowfish, TEA, RC6 and AES algorithms, respectively. While Table 7-10 show the correlation after applying proposed system with Blowfish, TEA, RC6 and AES as function in the BK-Cube network design.

Table 3: The C between original images and their corresponding encrypted images using blowfish

Images	C_{RR}	C_{GG}	C_{BB}
A	0.1461	0.1340	0.1252
Nike	0.1068	0.1024	0.1005
Duck	0.0683	0.0776	0.0794
Lena	0.0051	0.0020	0.0007

Table 4: The C between original images and their corresponding encrypted images using tea

Images	C_{RR}	C_{GG}	C_{BB}
A	0.0230	0.0905	0.2069
Nike	0.0391	0.0182	0.0817
Duck	0.0862	0.1026	0.0916
Lena	0.0008	0.0032	-0.0035

Table 5: The C between original images and their corresponding encrypted images using RC6

Images	C_{RR}	C_{GG}	C_{BB}
A	0.0078	0.0071	0.0073
Nike	0.0250	0.0265	0.0138
Duck	0.0078	0.0021	0.0093
Lena	-0.0620	-0.0581	0.0074

Table 6: The C between original images and their corresponding encrypted images using AES

Images	C_{RR}	C_{GG}	C_{BB}
A	0.0002	0.0008	0.0282
Nike	0.0020	0.0018	0.0096
Duck	-0.0047	0.0052	0.0036
Lena	-0.0028	-0.0038	-0.0026

Table 7: The C between original images and their corresponding encrypted images using proposed system with blowfish

Images	C_{RR}	C_{GG}	C_{BB}
A	-0.0169	-0.0022	0.0086
Nike	0.0063	-0.0056	0.0046
Duck	0.0051	-0.0019	0.0028
Lena	3.4122e-004	0.0009	-0.0010

Table 8: The C between original images and their encrypted images using proposed system with tea

Images	C_{RR}	C_{GG}	C_{BB}
A	0.0063	-0.0043	0.0086
Nike	0.0012	0.0021	0.0046
Duck	-0.0051	-0.0083	0.0008
Lena	0.0007	-0.0008	-0.0010

Table 9: The C between original images and their encrypted images using proposed system with RC6

Images	C_{RR}	C_{GG}	C_{BB}
A	-0.0169	-0.0022	-0.0086
Nike	0.0007	-0.0091	0.0006
Duck	0.0018	-0.0004	-0.0090
Lena	-0.0054	-0.0046	--0.0010

Table 10: The C between original images and their encrypted images using proposed system with AES

Images	C_{RR}	C_{GG}	C_{BB}
A	-0.0391	-0.0073	-0.0824
Nike	0.0063	-0.0056	0.0046
Duck	0.0051	-0.0019	0.0028
Lena	-0.0061	0.0029	-0.0010

Samples of the test results of correlation coefficient of the proposed system are shown in Tables 7-10. The

Table 11: The entropy values for different cipherd images with Blowfish

Images	Plain images	Cipher images
A	2.1411	5.3995
Nike	0.1205	3.1410
Duck	2.3445	5.5249
Lena	7.7260	7.9972

Table 12: The entropy values for different cipherd images with tea

Images	Plain images	Cipher images
A	2.1411	4.7337
Nike	0.1205	4.4549
Duck	2.3445	5..7243
Lena	7.7260	7.5321

Table 13: The entropy values for different cipherd images with RC6

Images	Plain images	Cipher images
A	2.1411	5.5230
Nike	0.1205	3.1574
Duck	2.3445	5.6789
Lena	7.7260	7.6348

Table 14: The entropy values for different cipherd images with AES

Images	Plain images	Cipher images
A	2.1411	6.8463
Nike	0.1205	5.0129
Duck	2.3445	6.8682
Lena	7.7260	7.8762

results of correlation coefficient shown in these tables are very small indicates that the plain images and their corresponding cipher images are completely uncorrelated with each other compared with the results which are shown in Table 3-6.

Information entropy: The lack of clarity and indeterminate are the primary goals of image encryption. This limit can be reflected by one of the most common used theoretical measurement of entropy information. Entropy information expresses a degree of uncertainty in the system and defines as follows:

$$H = -\sum_{k=0}^{G-1} P(k)\log_2(P(k)) \quad (2)$$

Where:

H = The entropy
G = The gray scale (= 255)
P (k) = The probability of the occurrence of symbol k

Tables 11-14 show the entropies between original images and ciphered images using Blowfish, TEA, RC6 and AES algorithms respectively. While Table 15-18 show the entropy after applying proposed system with Blowfish, TEA, RC6 and AES as function in the BK-Cube network design.

From the above results, the proposed algorithm get higher entropy compared with previous algorithms. Also, by splitting the input image into a number of subblocks made performance even better.

Table 15: The entropy values for different cipherd images of proposed system with Blowfish

Images	Plain images	Cipher images
A	2.1411	7.7421
Nike	0.1205	7.682
Duck	2.3445	7.7781
Lena	7.7260	7.9923

Table 16: The entropy values for different cipherd images of proposed system with tea

Images	Plain images	Cipher images
A	2.1411	7.6421
Nike	0.1205	7.5821
Duck	2.3445	7.7281
Lena	7.7260	7.9823

Table 17: CR The entropy values for different cipherd images of proposed system with RC6

Images	Plain images	Cipher images
A	2.1411	7.9823
Nike	0.1205	7.9735
Duck	2.3445	7.9841
Lena	7.7260	7.9965

Table 18: The entropy values for different cipherd images of proposed system with AES

Images	Plain images	Cipher images
A	2.1411	7.9923
Nike	0.1205	7.9835
Duck	2.3445	7.9945
Lena	7.7260	7.9967

CONCLUSION

In this study an enhanced algorithm for image encryption is presented by using improving four encryption algorithms Blowfish, TEA, RC6 and AES to encrypt color images. Two evaluating measuring factors are considered in addition to visual inspection. Based on conducted results; The proposed system with all four enhanced algorithms has been offered high encryption quality. The proposed system enhanced the security level of the encrypted images by reducing the correlation among image elements while increasing its entropy value by decreasing the mutual information among the encrypted image variable. The simulation results presented that AES has superior performance when it is used as function in the proposed system than encryption algorithms which are used. To date, AES has not shown any security week. Therefore, it is considered as an excellent candidate as a standard encryption algorithm for image encryption. According to the conducted results we concluded that the proposed system is expected to be useful for real-time image encryption and transmission applications. This research can be further extended by increasing block size and rounds.

REFERENCES

Ali, Y.H. and H.A. Ressan, 2016. Image encryption using block cipher based serpent algorithm. Eng. Technol. J., 34: 278-286.

Alshahrani, A.M. and S. Walker, 2015. New approach in symmetric block cipher security using a new cubical technique. Intl. J. Comput. Sci. Inf. Technol., 7: 69-75.

Gonzales, R.C. and R.E. Woods, 2002. Digital Image Processing. 2nd Edn., Pearson, London, England, UK., ISBN:978-81-7758-168-3, Pages: 793.

Helal, B.H. and A.T. Hashim, 2010. Measurement of encryption quality of bitmap images with RC6 and two modified version block cipher. Eng. Technol. J., 28: 5603-5613.

Hernandez, J.C., J.M. Sierra, A. Ribagorda, B. Ramos and J.C. Mex-Perera, 2001. Distinguishing TEA from a random permutation: Reduced round versions of TEA do not have the SAC or do not generate random numbers. Proceedings of the 8th IMA International Conference on Cryptography and Coding, December 17-19, 2001, Springer, Cirencester, England, UK., ISBN:978-3-540-43026-1, pp: 374-377.

Padate, R. and A. Patel, 2015. Image encryption and decryption using AES algorithm. Intl. J. Electron. Commun. Eng. Technol., 6: 23-29.

Rivest, R.L., M.J.B. Robshaw, R. Sidney and Y.L. Yin, 1998. The RC6™ block cipher. J. Comput. Syst., 1: 1-21.

Schneier, B., 1996. Applied Cryptography: Protocols, Algorithms and Source Code in C. 2nd Edn., John Wiley & Sons, Hoboken, New Jersey, USA., ISBN:9780471128458, Pages: 758.

Shrivastava, A. and L. Singh, 2016. An efficient RC6 based image cryptography to enhance correlation and entropy. Intl. J. Comput. Appl., 139: 42-49.

Singh, H., D.N. Dhillon and S.S. Bains, 2013. A new approach for image cryptography techniques. Intl. J. Comput. Organ. Trends, 3: 404-408.

Sudha, S.S. and S. Divya, 2015. Cryptography in image using blowfish algorithm. Intl. J. Sci. Res., 4: 1289-1291.